### Capítulo 13 - Administração de Usuários

Saber administrar os usuários do sistema é ter total poder sobre o sistema de permissionamento de arquivos e diretórios. Nesse capítulo vamos nos aprofundar nesses assuntos.





## **Objetivos**

- Descobrir o sistema de permissionamento;
- Gerenciar usuários e grupos;
- Entender o papel da "umask" e das permissões especiais;

### Começando pelo.... começo

- Usuário Administrador;
- Usuário de Sistema;
- Usuários Comuns;

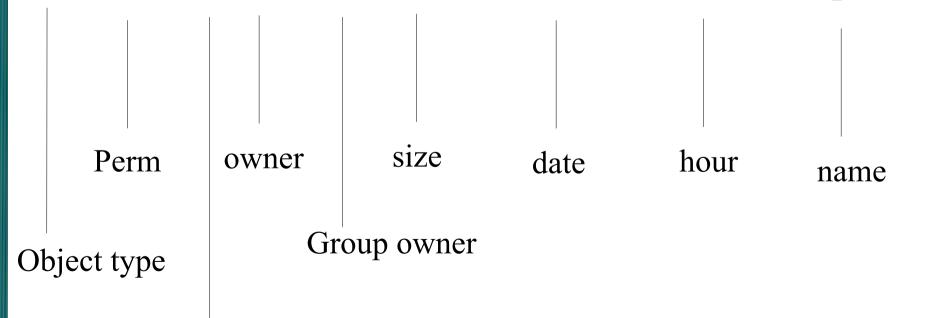
#### Permissões ...

- Conhecendo novos horizontes...
- UGO
- OCTAL

### Recapitulando

\$Is -I /etc/passwd

-rw-r--r-- 1 root root 1528 2008-10-28 17:41 /etc/passwd



Nº of related objects

#### Visualisando e entendendo.

- rw- r-- r-U G O read
S R T write
E O H write
R U E execute



Conhecer o sistema de permissionamento é fundamental para seu dia-a-dia.

### Atribuindo permissões

chmod

<u>Grupos</u>	<u>Operadores</u>	<u>Perms</u>	
u – user	+	r	
g – grupo	_	W	
o – outros	=	X	
a – todos			

### **Exemplos**

chmod a+x arquivo

chmod u+rw,g-w diretório

chmod a=rw arquivo

chmod u+w,g-w,o-rwx arquivo

#### Facilitando com o modo OCTAL

r=4	w=2	x=1	Octal	Perm
0	0	0	0	
0	0	1	1	X
0	1	0	2	-W-
0	1	1	3	-WX
1	0	0	4	<b>r</b>
1	0	1	5	r-x
1	1	0	6	rw-
1	1	1	7	rwx

#### OCTAL >>> 0-7



Para o seu dia-a-dia é muito mais prático aprender o modo octal de permissionamento UNIX. De quebra, memoriza-o para prova da LPI. Sempre lembre dos valores:

$$r=4 w=2 x=1$$



#### Então

- chmod 644 arquivo
- chmod 500 diretório
- chmod 666 arquivo

MAS NUNCA!

chmod 777 / -R





### Definindo dono e grupo dono

- chown
- chgrp

#### MiiiiauUUUUU!!



Usando o "chown" de maneira prática e rápida:

\$ chown user.user arq2

### **Arquivos importantes**

/etc/passwd

/etc/shadow

/etc/group

/etc/gshadown

#### Pwconv e pwunconv



Senhas de sombra podem ser ativadas e desativadas através dos comandos:

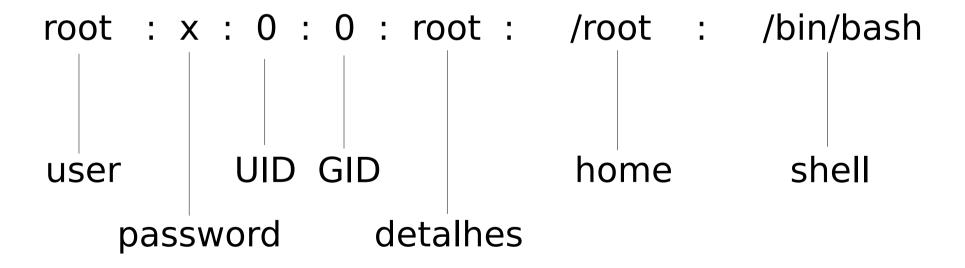
**\$ pwconv** Ativa

**\$ pwunconv**Desativa

Por que ativar ... análise de permissões ;;;

### O arquivo de Senhas

getent passwd



### Comandos para a administração

- ▶ id
- finger
- users
- who
- ► W

#### Last logged users



Para vermos os últimos usuários logados no sistema, podemos utilizar o comando:

\$ last

#### Adicionando e removendo usuários

- adduser X useradd
- userdel

#### adduser.conf



Configurar a adição de usuários através do arquivo de configuração "adduser.conf" otimiza diversas opções que deixam de ser configuras manualmente, como adição do usuário em grupos ou mesmo definição de QUOTA

/etc/adduser.conf

#### userdel -r



Para não gerar heranças de diretórios no sistema sempre apague o diretório "home" na exclusão do usuário. Para isso:

\$ userdel -r user

### Adcionando e removendo grupos

- groupadd x addgroup
- groupdel
- groups

### Gerenciando Grupos

- gpasswd
- usermod

#### Falando de umask

Permissões de criação padrão

Padrão 022

Diretórios devem sempre ser diminuidos de 777.Por exemplo:

777
 <u>015 - umask definida</u>
 765 Permissões padrões do sistema

#### Falando de umask

- Atenção especial para arquivos;
- Quando par, diminuir de 6;
- Quando impar, diminuir de 7;

677

015 - umask definida

662 Permissões padrões do sistema

#### Linux Essentials – 450 – Slide - 26

## Manipulando Hardware e dispositivos

#### **UMASK**



Apesar de muitas divergências nesse assunto, o cálculo de "umask" é bem simples, podendo ser pensado de duas formas:

Fórmula (Par e impar)

e

Tirando permissões de exec.

### Permissões especiais

	SUID	SGID	Sticky
Aonde	U	G	Ο
Como	S s	S s	T t
Quanto	4	2	1

Exemplos
SUID => -rwsrw-rwSGUI => -rwxrwSrwx
Sticky => -rwxrwxrwt

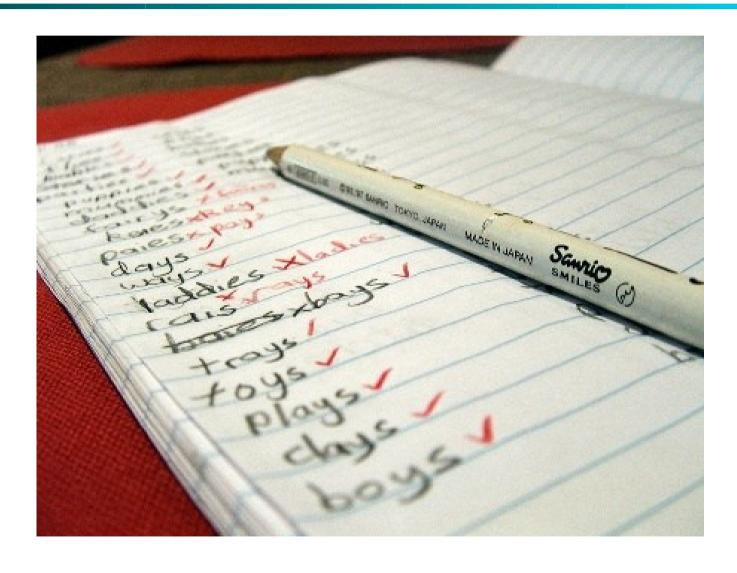
chmod 4766 arq
chmod 2767 arq
chmod 1777 arq

### Permissões especiais



O uso da permissão "SUID bit" deve ser feito com muita cautela, pois com uma permissão atribuída de maneira errada a um binário importante, pode-se comprometer totalmente a segurança do sistema.

### **Exercícios:**



### Respostas dos Exercícios

- 1. Restrições na permissão de outros tornam o arquivo mais seguro, evitando um ataque por "brute force".
- 2. É um exigência do sistema, precisamos dele para criar qualquer tipo de objeto.
- 3. Administradores, sistema, comum
- 4. Evitar problemas de herança
- 5. getent passwd
- 6. gpasswd adicionausermod deixa teste1 somente no grupo cdrom
- 7. rw-r--r--, rwxr-r-x,
- 8. dir=765 arqs=664

### Conclusão

Temos o domínio da manipulação de usuários e arquivos do sistema.

Iremos estudar agora a Administração do shell.